TISAX® Assessment Report

Initial Assessment

ScioSense B.V.

S471X2

AL3KR6-1

27.09.2023

Version 1.0

Conducted by

DNV Business Assurance Zertifizierung GmbH

Wolbeckstr. 25

45329 Essen, Germany

Initial Remarks

This Assessment Report and its underlying assessment was created by qualified experts of an TISAX audit provider. It expresses professional judgement of the effectiveness of control procedures based on the current state of implementation and in accordance to the Audit Provider Criteria and Assessment Requirements (ACAR) of the Trusted Information Security Assessment Exchange (TISAX) as defined and published by ENX Association at the time of the issuance of this report.

The Trusted Information Security Assessment Exchange (TISAX) is operated and governed by ENX Association. TISAX was created to provide commonly accepted assessments based on the ISA control catalogue conducted by trustworthy competing audit providers. Detailed information about TISAX can be found at http://www.enx.com/tisax/.

This Assessment Report is intended exclusively for use within TISAX. All distribution or exchange of TISAX Assessment Results must follow the rules for information exchange established for TISAX Participants and TISAX Audit Providers within the applicable TISAX agreements and guidelines.

No exchange of TISAX Assessment Results outside the defined TISAX information exchange proceedings or exchange with third parties outside the TISAX shall take place. Please be aware that certain rights provided by the applicable TISAX legal framework may cease when exchanging TISAX Assessment Results outside the set guidelines.

The underlying assessment engagement is not designed to detect all weaknesses in control procedures because it is not performed continuously throughout the period and the checks performed on the control procedures are on a sample basis. As such, even though checks are conducted with due diligence, misstatements due to errors or fraud may occur and go undetected.

Additionally, the assessment was based on the situation at the day of the assessment and does not account for any changes in the future. Any projections of any evaluation to future periods are subject to the risk that the report may become inadequate because of changes in conditions, or that the level of compliance with the policies or procedures may deteriorate.

Report Structure

This report is structured as follows:

A. Assessment Related Information
B. Summarized Results
C. Assessment Result Summary
D. Maturity Levels of ISA (Result Tab)
E. Detailed Assessment Results

The structure and headlines reflect different levels of possible disclosure regarding its content towards other TISAX Participants.

Starting with general information about the assessment (A. Assessment-Related Information), it spans from a summary of results (B. Summarized Results, C. Assessment Result Summary) to the very details of the assessment (D. Maturity Levels of ISA and E. Detailed Assessment Results).

A. Assessment Related Information

A.1 Assessment Scope

TISAX® Scope-ID	S471X2
Scope Type	☒ Standard Scope 2.0 *The TISAX Scope defines the scope of the assessment. The assessment includes all processes, procedures and resources under responsibility of the assessed organization that are relevant to the security of the protection objects and their protection goals as defined in the listed assessment objectives at the listed locations.* *The assessment is conducted at least in the highest Assessment Level listed in any of the listed Assessment Objectives. All assessment criteria listed in the listed assessment objectives are subject to the assessment.*
Assessment Objectives	☒ Handling of Information with High Protection Level ☐ Handling of Information with Very High Protection Level ☐ Handling of Prototype Components and Parts ☐ Handling of Prototype Vehicles ☐ Use of Test Vehicles ☐ Events and Photo Shootings with Objects in Need of Protection ☐ Handling of Personal Data according to article 28 GDPR (“processor”) ☐ Handling with Special Categories of Personal Data (article 9 GDPR) according to article 28 GDPR (“processor”)
Assessment Requirements	ACAR – TISAX Specification of Assessment Version 2.1: Family-ID: ISA, Version 5.0

A.2 Assessed Locations

Company Name	Address	Location-ID	Contact Person
ScioSense B.V.	High Tech Campus 10 5656 AE Eindhoven Netherlands	L1XPZ4	Peter Hoppenbrouwers +31 (6)89934311 , peter.hoppenbrouwers@sciosense.com
Sciosense Germany GmbH	Gerhard-Kindler Strasse 8 72770 Reutlingen Germany	LV2ZTV	Peter Hoppenbrouwers +31 (6)89934311 , peter.hoppenbrouwers@sciosense.com
Sciosense Germany GmbH	Friedrich-List-strasse 4 76297 Stutensee Germany	LNV6V9	Peter Hoppenbrouwers +31 (6)89934311 , peter.hoppenbrouwers@sciosense.com
Sciosense Italy Srl	Via Mario Giuntini 63 56021 Navacchio	L3W7VP	Peter Hoppenbrouwers

	Italy		+31 (6)89934311 , peter.hoppenbrouwers@sciosense.com
Sciosense JV	Room 1002, Building 1, Sandhill Plaza, No. 2290 Zuchongzhi Road Zhangjiang Hi-Tech, Pudong New District Shanghai China 201203	LN7X12	Peter Hoppenbrouwers +31 (6)89934311 , peter.hoppenbrouwers@sciosense.com
ScioSense Technology (Jinan) Co., Ltd.	Rm 401, Building 1, No. 7558, Century Avenue, Zhangqiu District Jinan Shandong China 250220	LFX273	Peter Hoppenbrouwers +31 (6)89934311 , peter.hoppenbrouwers@sciosense.com

The auditor confirms that all information above is verified to be accurate.

A.3 Initial Assessment

TISAX® Assessment-ID	AL3KR6-1
Assessment Level	AL2
Assessment Method	☒ Plausibility check of self-assessment using evidences and documentation ☐ Detailed evaluation of evidence ☒ Interviews with persons involved in the processes of the auditee ☐ On-site Inspection ☐ Video based remote site inspection
Date of Kick-Off Meeting	09.05.2022
Date of Opening Meeting	18.09.2023
Date of Closing Meeting (Effective Date)	20.09.2023
Consent of Auditee	The auditee ☒ unqualifiedly agrees on the documented conclusions. ☐ qualifiedly agrees on assessment conclusions (auditee's dissenting comments are included and marked in the report).

Authors

Auditor
Stephan Laske

Essen, 27.09.2023

Stephan Laske

Name of Auditor
DNV Business Assurance Zertifizierung GmbH

B. Summarized Results

B.1 Initial Assessment

AL2: Based on the observations during the initial assessment the overall assessment of the scope is:

☒ Conform

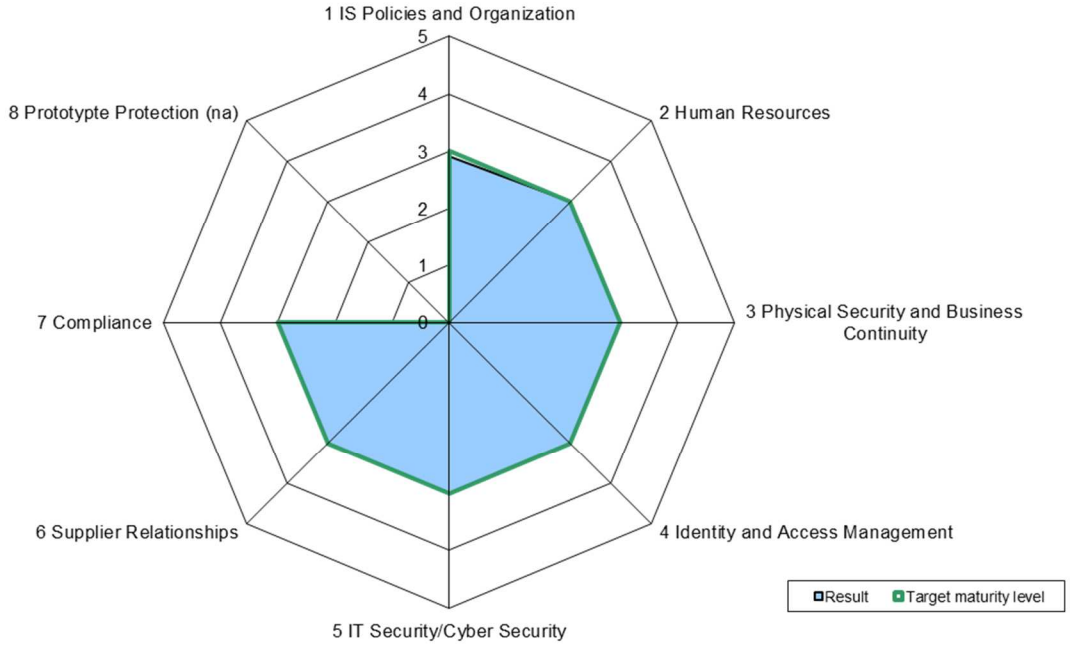
In total, 0 major and 0 minor non-conformities to the assessed catalogue were identified.

After the initial assessment an average maturity level of 2,98 was calculated.

C. Assessment Result Summary

C.1 Initial Assessment

The individual areas of the initial maturity levels can be found in the spider web diagram below.



The major and/or minor non-conformities, as applicable, were identified in the following Areas:

No.	Area	Number of major non-conformities	Number of minor non-conformities
1	IS Policies and Organization	0	0
2	Human Resources	0	0
3	Physical Security and Business Continuity	0	0
4	Identity and Access Management	0	0
5	IT Security / Cyber Security	0	0
6	Supplier Relationships	0	0
7	Compliance	0	0
8	Prototype Protection	N/A	N/A
9	Data Protection	N/A	N/A

D. Maturity Levels of ISA (Result Tab)

D.1 ISMS

Based on the current status of implementation, the following maturity levels result for the controls listed in the ISMS Area:

No.	Control Question	Target maturity level	Result
1	***IS Policies and Organization***		
1.1	***Information Security Policies***		
1.1.1	To what extent are information security policies available?	3	**3**
1.2	***Organization of Information Security***		
1.2.1	To what extent is information security managed within the organization?	3	**3**
1.2.2	To what extent are information security responsibilities organized?	3	**3**
1.2.3	To what extent are information security requirements taken into account in projects?	3	**3**
1.2.4	To what extent are responsibilities between external IT service providers and the own organization defined?	3	**3**
1.3	***Asset Management***		
1.3.1	To what extent are information assets identified and recorded?	3	**2**
1.3.2	To what extent are information assets classified and managed in terms of their protection needs?	3	**3**
1.3.3	To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	3	**3**
1.4	***IS Risk Management***		
1.4.1	To what extent are information security risks managed?	3	**3**
1.5	***Assessments***		
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	3	**3**
1.5.2	To what extent is the ISMS reviewed by an independent entity?	3	**3**
1.6	***Incident Management***		
1.6.1	To what extent are information security events processed?	3	**3**

2	***Human Resources***		
2.1.1	To what extent is the suitability of employees for sensitive work fields ensured?	3	**3**
2.1.2	To what extent is all staff contractually bound to comply with information security policies?	3	**3**
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	3	**3**
2.1.4	To what extent is teleworking regulated?	3	**3**
3	***Physical Security and Business Continuity***		
3.1.1	To what extent are security zones managed to protect information assets?	3	**3**
3.1.2	To what extent is information security ensured in exceptional situations?	3	**3**
3.1.3	To what extent is the handling of supporting assets managed?	3	**3**
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	3	**3**
4	***Identity and Access Management***		
4.1	***Identity Management***		
4.1.1	To what extent is the use of identification means managed?	3	**3**
4.1.2	To what extent is the user access to network services, IT systems and IT applications secured?	3	**3**
4.1.3	To what extent are user accounts and login information securely managed and applied?	3	**3**
4.2	***Access Management***		
4.2.1	To what extent are access rights assigned and managed?	3	**3**
5	***IT Security/Cyber Security***		
5.1	***Cryptography***		
5.1.1	To what extent is the use of cryptographic procedures managed?	3	**3**
5.1.2	To what extent is information protected during transport?	3	**3**
5.2	***Operations Security***		
5.2.1	To what extent are changes managed?	3	**3**

5.2.2	To what extent are development and testing environments separated from operational environments?	3	**3**
5.2.3	To what extent are IT systems protected against malware?	3	**3**
5.2.4	To what extent are event logs recorded and analyzed?	3	**3**
5.2.5	To what extent are vulnerabilities identified and addressed?	3	**3**
5.2.6	To what extent are IT systems technically checked (system audit)?	3	**3**
5.2.7	To what extent is the network of the organization managed?	3	**3**
5.3	***System acquisitions, requirement management and development***		
5.3.1	To what extent is information security considered in new or further development of IT systems?	3	**3**
5.3.2	To what extent are requirements for network services defined?	3	**3**
5.3.3	To what extent is the return and secure removal of information assets from external IT services regulated?	3	**3**
5.3.4	To what extent is information protected in shared external IT services?	3	**3**
6	***Supplier Relationships***		
6.1.1	To what extent is information security ensured among suppliers and cooperation partners?	3	**3**
6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	3	**3**
7	***Compliance***		
7.1.1	To what extent is compliance with regulatory and contractual provisions ensured?	3	**3**
7.1.2	To what extent is the protection of personal data taken into account when implementing information security?	3	**3**

D.2 Handling of Prototypes

The module has not been assessed.

D.3 Data Protection

The Data Protection Module is not following the ISA maturity levels and therefore not listed here.

E. Detailed Assessment Results

1 IS Policies and Organization

1.1 Information Security Policies

1.1.1 To what extent are information security policies available?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Sciosense has created a information security policy & Procedures that is customized to the needs, goals and strategy of Sciosense organization. This policy is documented, made available for review (if applicable) on Sciosense Intranet and communicated in Sciosense Townhall's meetings where all staff members are present. The documentation (Policy & Procedure (*also delvered) has been approved by Sciosense Management and the security counsil. This document describes the opbjectives, responsibilities, changes and reviews sequence. (Reviews as task in ISMS) The information security policy is made available to employees and to relevant business partners when needed.(COC/ OCO IT = Intranet & Cognidox) For external parties are NDA's provided when needed.* **The following documents were checked during the assessment:** • *Vision & Policy, Code of Conduct, Processing Agreements* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.2 Organization of Information Security

1.2.1 To what extent is information security managed within the organization?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Follow up by Security Committee; monthly meetings, minutes,Management Review: 2x/year. 'Information security is a strategic objective within Sciosense because IP security , Data integrity & continuity of our business is a big part of our organization. Since we are still a "young" organization, we first focused on the interpretation (description) of the security policies and procedures. Sciosense has setup a control mechanisms ISMS called Base27. The scope is determined, and requirements are drafted under (visopn & policy : SC-000112-FM – ScioSense Information Security Management System). The ISMS is fully based on ISO 27001 and provides the organizational management with suitable monitoring and control. Reviewing of the ISMS is done (will be done) by the manager ISM & SO.* **The following documents were checked during the assessment:** • *SC-000112-FM – ScioSense Information Security Management System* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.2.2 To what extent are information security responsibilities organized?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Within Sciosense the responsibilities for information security are clearly stated, appointed and described. Manager ISMS & Security Officer are official appointed, responsibilities are defined and people are qualified for their task. The persons are known within the organization and organization of our customers and/or partners (If applicable)* **The following documents were checked during the assessment:** • *SC-000112-FM – ScioSense Information Security Management System* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.2.3 To what extent are information security requirements taken into account in projects?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☐ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *We are using / taking into account our security policies within projects. Security Officer involved in projects that may affect Info Sec. Projects requirements of projects are assessed in the startup of an project. Risk management is conduct and security issues within the project organization are defined and addressed. Every project within Sciosense has a "supplier". In our supplier procedure BIA is be done to do a Risk management. Risk management is an always recurring part with our project organization and is reviewed frequently. Out of the BIA it will be clear if information security is part of a project.* **The following documents were checked during the assessment:** • *SC-000112-FM – ScioSense Information Security Management System.pdf* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.2.4 To what extent are responsibilities between external IT service providers and the own organization defined?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *For Sciosense, IT vendors that are involved in any information security related topics, NDA's and/ or contracts are in place that cover the relevant requirements and responsibilities. Also agreements are made about shared responsibilities and the implementation as such. IT Vendors and IT Sciosense are trained / monitored to accomplish their task. A list of all IT suppliers is maintained in base27 (ISMS) monitored and managed . (from the outcome of the BIA, SLA. ISO certification , DPA are provided).* **The following documents were checked during the assessment:** • *SC-000456-FM-5-Sciosense Supplier selection checklist* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.3 Asset Management

1.3.1 To what extent are information assets identified and recorded?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☒ Interviews ☐ Onsite inspection ☒ Document inspection ☒ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *Main assets (information systems & HW Assets as important information) are registered in a detailed way including BIA. (IS) Every asset has an owner. (Check for IS are done regular) 'Important Sciosense Assets (IP) are kept & managed in several IT systems used by Sciosense. These systems are under responsibility of IT and Keyusers for every important assets groups. The keyusers are also responsible for the information (assets) stored in that system. The inventory as also the used systems are reviewed on a regular bases for access and use. The information assets used/ stored in these systems are identified & recorded as IP. Also shown with different icons on storage systems.*

The following documents were checked during the assessment:

- *Base27 tool overview*

The following MUST-requirements have been verified during the assessment:

- Implementation check, whether information assets of critical value to the organization are identified and recorded.
- Implementation check, whether a person responsible for these information assets is assigned.
- Implementation check, whether the supporting assets processing the information assets are identified and recorded.
- Implementation check, whether a person responsible for these supporting assets is assigned.

The following SHALL-requirements have been verified during the assessment:

- Implementation check, whether an inventory of critical information assets exists.
- Implementation check, whether each critical information asset is assigned the respective supporting assets.
- Implementation check, whether the inventory is reviewed at regular intervals.

The following further information was documented during the assessment:

Information assets and supporting assets are listed in Base27. ScioSense presented their asset inventory within the Base27 tool. ScioSense list their important business processes within Cognidox (DMS).

Finding

1.3.1.1. The overview of critical information assets / supporting assets / business processes is splitted into several areas within Base27 / cognidox.

☐ Major non-conformity ☐ Minor non-conformity ☒ Observation ☐ Room for improvement

1.3.2 To what extent are information assets classified and managed in terms of their protection needs?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Sciosense has defined a Data Classification Matrix in the Sciosense ISMS - 'BIA executed for all information systems and measures taken. ' A consitent scheme for the classification of informations assets with regard to the protection goal of configentiality is made and documented in Base27 (SC-002013-PR Information classification matrix and Data handling guide.)* **The following documents were checked during the assessment:** • *SC-002013-PR Information classification matrix and Data handling guide* **The following MUST-requirements have been verified during the assessment:** • Control of documents, whether a consistent scheme for the classification of information assets with regard to the protection objective of confidentiality is available. • Control of documents, whether evaluation of the identified information assets is carried out according to the defined criteria and assigned to the existing classification scheme. • Control of documents, whether requirements for the handling of supporting assets (e.g. marking, correct handling, transport, storage, return, deletion/disposal) depending on the classification of the information assets exist and are applied. **The following SHALL-requirements have been verified during the assessment:** • Explanation from the participants that the protection objectives of integrity and availability are taken into consideration. **The following further information was documented during the assessment:** ScioSense developed a process like a tool to make it easier for employess to classify their information.
Finding
Based on the observations, no deviation was found.

1.3.3 To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Contractual requirement's are in place as NDA, and contracts to avoid unauthorized access. In Sciosense ERP the roles are divided and separations of duty's (SOD: Segregation of Duties) are taken into account. (Access Matrix 1 & 2). ScioSense is in relation with only one IT Supplier named LEITWERK, here are default measurements taken like BIA, risk analysis, contracts etc. Other IT Supplier are used only for project relevant tasks, next to contracts/agreements the access is monitored in realtime.* **The following documents were checked during the assessment:** • *Access Matrix 1 & 2* • *SC-002018-PR Internet guidelines & process.pdf* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.4 IS Risk Management

1.4.1 To what extent are information security risks managed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☒ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Risk Management implemented: described in Vision&Policy Ch. 6.1. Managed by Security Committee (CAB) 'information security and risk management are part of the Sciosense enterprise risk management framework, which is documented within Vision& Policy. Within Sciosense we have a Risk manager who is responsible for the timely detection, assessment and management of risks in order to achieve the protection objectives of information security.(CFO = role of Risk-manager within SC/CAB)* • *Risk assessments take place at regular intervals in consultation with the security council in the CAB, and as well as on any relevant occassion(s) depending on the need. Incidents and the information security risks are documented within which the risk manager is responsible for each information security risk but where actions to be taken can be delegated to members of the security council. (SO).* • *The information security risks are documented within the ISMS. "* **The following documents were checked during the assessment:** • *(base27)/ risks* **The following MUST-requirements have been verified during the assessment:** • Control of documents, whether risk assessments are carried out both at regular intervals and in response to events. • Control of documents, whether information security risks are assessed in a suitable manner according to e.g. probability of occurrence and potential damage. • Implementation check, whether information security risks are documented. • Implementation check, whether a responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks. **The following SHALL-requirements have been verified during the assessment:** • Control of documents, whether a procedure to identify, assess and address information security risks within the organization is in place. • Control of documents, whether criteria for the assessment and handling of information security risks exist. • Implementation check, whether measures for handling information security risks and the persons responsible for these are specified and documented. • Implementation check, whether a plan of measures or an overview of their state of implementation exists.

- Control of documents, whether in case of changes to the environment (e.g. organizational structure, location, changes to regulations), reassessment is carried out in a timely manner.

The following further information was documented during the assessment:

ScioSense presented there is risk assessment policy and their risks overview and their measure list.

Finding

Based on the observations, no deviation was found.

1.5 Assessments

1.5.1 To what extent is compliance with information security ensured in procedures and processes?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Annual review of all policies: planned in Operational Planning, Internal Audit. 'The time intervals (Schedule) for reviewing Sciosense policies & procedures are verified on a regular bases . (Check Base27 ISMS, Management review ISMS, policy's & procedures. 2 times a year. In terms of GDPR, HR regularly checks compliance to all department managers. Tracked via Base 27. New Employess and external Contractors are introduced to the policies when starting at ScioSense, 4 Times a Year during the Site Check (Base27) some employees are tested about the awareness of the policies.* **The following documents were checked during the assessment:** • *Base27 ISMS, Management review ISMS, policy's & procedures* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.5.2 To what extent is the ISMS reviewed by an independent entity?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *External consultant used during implementation, annual review/validation of the Tisax internal en external audit planned in the operational plan (check).* **The following documents were checked during the assessment:** • *operational plan (check)* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

1.6 Incident Management

1.6.1 To what extent are information security events processed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Incidents primarily processed by service desks; tickets made in te sciosense Helpdesk,. Incidents followed up & evaluated by SO/ Security Committee. Also a data breach procedure is in place.. A procedure exist for reporting and recording the information per event. (Data Breaches) In this procedure the follwing aspects are considered: The event (what), How to infom, how to react, how to escalte (and to whom). How to analyze, how to prevent furture or similair events. (PDCA) Important Security events are always part of the CAB? security councel meeting.* **The following documents were checked during the assessment:** • *SC-000112-FM – ScioSense Information Security Management System.pdf* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

2 Human Ressources

2.1.1 To what extent is the suitability of employees for sensitive work fields ensured?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Onboarding proces including screening to the extent required for a position. 'Before starting the recruitment, the requirements for the position regarding job profile are determined and used as a basis in the hiring process. The personal suitability of potential employees is verified by simple methods. The application process consists of at least 2 interviews. On entry, the identity of a new employee is verified by checking the passport or ID of the employee. This document is saved in the personnel file of the employee. For key roles we ask for a letter of good behavior from public registers.* **The following documents were checked during the assessment:** • *SC-000112-FM – ScioSense Information Security Management System.pdf* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

2.1.2 To what extent is all staff contractually bound to comply with information security policies?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Code of Conduct (IT users + Normal), Labour contract. 'With every new employee, a contractual confidentiality clause is being agreed upon in the employment contract (which also stays in place after the end of the contract), as well as the employees obligation to comply to all regulations and policies as set up by the employer. For Sciosense, in the employee handbook and guidelines reference is made to disciplinairy meassures.* **The following documents were checked during the assessment:** • *employee handbook and guidelines reference* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

2.1.3 To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *Town Hall meetings, phished academy, presentation (whitepapers) 'Frequently, In Sciosense Townhall meetings Security is a topic of attention to inform and grow awareness within Sciosense employees. Also whitepapers about different security topics are provided trough Sciosense Intranet. In these townhall session we make people aware of ScioSense security policy and it existence an how to react on malware/ phishing emails and how Security is organized within Sciosense. Sciosense make use of the Phished platform for all theire employees to raise security awareness. Participation in training and awareness measures are regular checked. Site check is used to interview some people about there awareness* **The following documents were checked during the assessment:** • *SC-000112-FM – ScioSense Information Security Management System.pdf* • *Awareness document (Awareness concept)* **The following MUST-requirements have been verified during the assessment:** • Implementation check, whether employees are trained and made aware. **The following SHALL-requirements have been verified during the assessment:** • Control of documents, whether a concept for awareness and training of employees is prepared that include some basic aspects. • Control of documents, whether the Information security policy is part of the training. • Control of documents, whether the reporting of information security events is part of the training. • Control of documents, whether the reaction to occurrence of malware is part of the training. • Control of documents, whether the policies regarding user accounts and login information (e.g. password policy) are part of the training. • Control of documents, whether compliance issues of information security are part of the training. • Control of documents, whether requirements and procedures regarding the use of non-disclosure agreements when forwarding information requiring protection are part of the training. • Control of documents, whether the use of external IT services is part of the training. • Control of documents, whether target groups for training and awareness measures (e.g. new employees, administrators, employees having access to customer networks) are identified and taken into account in a training concept. • Control of documents, whether the concept has been approved by the responsible management.

- Control of documents, whether training and awareness measures are carried out both at regular intervals and in response to events.
- Implementation check, whether participation in training and awareness measures is documented.
- Control of documents, whether contact persons for information security are known to employees.

The following further information was documented during the assessment:

ScioSense uses an external service provider to offer IS awareness trainings. All locations in the scope have access to the online training. The trainings are seperated into small sessions.

From 145 employees (external employees are included) all of them are active users that participated at their online training.

ScioSense presented their awareness concept.

Finding

Based on the observations, no deviation was found.

2.1.4 To what extent is teleworking regulated?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Sciosense has the possibility for employees to telework (work from places out of the company) . Access from ""outside"" to the Sciosense network is only possible via a VPN. Our VPN has a 2 factor authentication so that only known devices in combination with a known user, can connect to the Sciosense network via the VPN. Sciosense also provides employees with guidelines (behavior/awareness) on how to work in public areas (e.g. during trips). Sciosense has taken protective measures if a Sciosense device is stolen. (Bitlocker,and Endpoint Management locking out a device and automatic formatting if the stolen device connects to the internet). Critical"" roles / colleagues are provided with ""read along filters"" to prevent viewing.* **The following documents were checked during the assessment:** *IT Code of Conduct,* • *chapter 6* • *Technical Security Policy* • *chapter 4 (A9),* • *chapter 4.3.2 (A.9.4.2)* • *chapter 7.3.3 (A.12.3.1)* • *chapter 8.1.4 (A.13.2.1)* • *chapter 9.1.2 (A.14.1.2)"* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

3 Physical Security and Business Continuity

3.1.1 To what extent are security zones managed to protect information assets?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"All Sciosense buildings/ area's are protected by access controls such as key readers. In these access keys access rights are established to different people (rolls) within the company for different area's within Sciosense. People known their access and limits. Visitor management is a part of the security policy . Within Sciosense we have a procedure how to handle and use, mobile, IT devices and access to a guest network is granted from, to, guest on a request bases to protect ScioSense for unauthorized access to our infrastructure. Physical Security document* • *Document is annually checked/updated"* **The following documents were checked during the assessment:** *Technical security procedure :* • *chapter 6 (A.11).* • *chapter 4.1.2 (A.9.1.2)* • *chapter 8.1.3 (A.13.1.3) How: IT Documentation/ Infrastructure/ Network* • *Under chapter 6 continuity plan:* • *(technical business continuity plan) chapter 2.3 network config.* • *Visitor registration policy* • *Visitor registration policy* **The following MUST-requirements have been verified during the assessment:** • Control of documents, whether a security zone concept including the associated protective measures based on the requirements for handling information assets is defined and documented. • Control of documents, whether security zones are specified and documented under consideration of terrains/buildings/rooms. This also includes delivery and shipping areas. • Control of documents, whether the defined protective measures are implemented. • Explanation from the participants that the code of conduct for security zones is known to all persons affected. **The following SHALL-requirements have been verified during the assessment:** • Control of documents, whether procedures for allocation and revocation of access rights are established.

- Control of documents, whether visitor management policies (including registration and escorting of visitors) are defined.
- Control of documents, whether policies for carrying along and using mobile IT devices and mobile data storage devices (e.g. registration before they are carried along, identification obligations) are defined and implemented.
- Implementation check, whether network/infrastructure components (own or customer networks) are protected against unauthorized access.

The following HIGH-requirements have been verified during the assessment:

- Control of documents, whether protective measures against simple overhearing and viewing are implemented.

The following further information was documented during the assessment:

ScioSense explained their physical security concepts. For most locations also an alarm system is available (this is documented in the physical security concept for every location).

Finding

Based on the observations, no deviation was found.

3.1.2 To what extent is information security ensured in exceptional situations?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☒ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Any disturbance , impact (Disaster or not) is identified & recorded in the Sciosense ISMS system. Sciosense minimized any single point of failures. All Single point of failures are identified / recorded. Sciosense infrastructure on every location is physical spliced (Redundancy, of Power, Servers, internet access, Backup of any media live & physically divided) so that in any case of a ""disaster"" college's of any ScioSense location can continue working. All Backup procedures are tested on a monthly bases. (DaSi & system checks) In case of an exceptional situation, ScioSense and its IT supplier have a contingency plan that is reviewed & tested on a regular basis, but at least once a year. The procedure for restoring the service (Fail-over/ Backup & retrieval) is tested regularly. (Once per month) Continuity Plan :* • *Plan is tested for IT aspects.* • *BHV organization on every site: annually audited (ISO9001)"* **The following documents were checked during the assessment:** *(SC-001787-PO - Sciosense Business Continuity Plan)* • *Technical security policy* • *chapter 7.3.3. (A.12.3.1)* **The following MUST-requirements have been verified during the assessment:** • Control of documents, whether possible exceptional situations are identified and recorded. • Implementation check, whether potentially endangered infrastructure components (e.g. access points, IT systems) are identified and recorded. • Control of documents, whether measures for limiting the impact of threats are identified and implemented. • Implementation check, whether for exceptional situations, information security aspects are taken into consideration in methods, processes and procedures. **The following SHALL-requirements have been verified during the assessment:** • Control of documents, whether emergency plans are defined and reviewed regularly. • Control of documents, whether physical security is generally maintained even in exceptional situations. • Control of documents, whether IT services are maintained even in exceptional situations. • Control of documents, whether recovery of data and applications by means of backup and redundancy concepts are existent.

- Control of documents, whether strategies to avoid permanent loss of information are defined.
- Control of documents, whether appropriate protective measures (e.g. fire alarm system, fire protection, water detectors) are implemented and regularly checked.
- Control of documents, whether a redundant media supply (e.g. power, communication connections) is available.
- Control of documents, whether information security is considered in business continuity management.
- Implementation check, whether information security measures for crisis situations are tested regularly.

The following further information was documented during the assessment:

In “Lansweeper” all critical infrastructure devices are registered.

Finding

Based on the observations, no deviation was found.

3.1.3 To what extent is the handling of supporting assets managed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"During the lifecycle (use), IT equipment, supporting the business, is protected against theft, loss or misuse. Therefore it is determined how Sciosense deals with devices during the lifecycle, including situations such as theft, transport or decommissioning of devices. In order to be able to manage this, an asset management system is in place"* **The following documents were checked during the assessment:** • *Technical Security Policy,* • *chapter 4 (A 9)* • *chapter 8.1.1 (13.1.1)* • *IT Code of Conduct* • *chapter 2, 4, 5.2.5, 5.2.7.* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

3.1.4 To what extent is the handling of mobile IT devices and mobile data storage devices managed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"During the lifecycle (use), IT equipment is protected against theft, loss or improper use. For example, devices are protected by a Bitlocker, AD managed passwords are used, devices are automatically erased in case of loss or theft, accounts are blocked or passwords are changed and privacy filters are applied where necessary. At the end of the life cycle of a device, the device is wiped and any sensitive data carriers are destroyed where necessary. In order to manage this, an Asset Management system (Lansweeper + Endpoint Management) is active where ALL Sciosense assets are managed/registered. For the use of Sciosense cell phones MDM (Mobile Device Management) will be deployed End 2023 TASK ISMS). The use of removable media (such as USB drives/SD cards) containing Sciosense data is not permitted outside Sciosense offices"* **The following documents were checked during the assessment:** • *Technical Security Policy,* • *chapter 3* • *chapter 4* • *chapter 5* • *Awareness training : How to work with Mobile Data Storage* • *(Phished Platform)* • *IT Code of Conduct* • *chapters 2, 5.2.7* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level.

• Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

4 Identity and Access Management

4.1 Identity Management

4.1.1 To what extent is the use of identification means managed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"The management of the use of identifiers (Badge/ Keys) are the responsibility of the different site managers/ office managers of the different Sciosense sites.When colleagues join the company, a means of identification based on his/her role is provided (as needed) in cooperation with the Human resource department. A signature is required for receipt and resources are recorded. Loss of a batch/key should be reported immediately so that corrective action can be taken (if necessary). Software tokens such as VPN/ access keys & certificates are (Removed only) controlled by the Active Directory where at loss (device) or at entry and exit tokens/certificates or User IDs are immediately deactivated. To accompany this, ScioSense has an on-off boarding procedure in place. Technical (IT) resources such as certificates / tokens are replaced at least once every two years. Twice a year, a check is done, to doublecheck the most importants access keys and considered if they are still needed/ in use"* **The following documents were checked during the assessment:** • *Technical Security Policy,* • *chapter 4 Policies for Access Security (A.9)* • *chapter 5 5. Cryptography (ISO27001-A.10)* • *Physical Security Policy,* • *HR (access badges etc.)* • *As above in the Technical Security Policy* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

4.1.2 To what extent is the user access to network services, IT systems and IT applications secured?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"Only ""securely"" identified (authenticated) Sciosense employees have access to IT systems/assets.*
- *When creating a Sciosense user the on-off boarding procedure is used to indicate, in consultation with the Human resource department, which role the new user will have within Sciosense. The new colleague/user is then created by IT within the Active Directory. Based on his / her role, the rights to certain resources / assets are then also given. (as needed) .(Also according the Authorization Matrix) By default, within Sciosense strong passwords are used and unauthorized access attempts are actively monitored, ""users"" are blocked from access in case of repeated wrong attempts to login and devices are locked after 10 minutes of inactivity or imidently by the motion sensor of the Laptops. The User accounts are sevured with conditional access policies and Multifactor Authentication. Unusual Logins are reported directly by our security systems. VPN access is performed using 2 factor authentication with device certificates linked to the user Authorisation matrix, (Base27 & SAP Auth. Matrix) "*

The following documents were checked during the assessment:

- *Onboarding/Offboarding Procedure.*
- *Procedure for access to sciosense datashares. (Sharepoint)*

- *Technical security policy:*
- *Chapter 4 : 4. Policies for Access Security (A.9)*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

4.1.3 To what extent are user accounts and login information securely managed and applied?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Access to information and IT systems is granted through validated user accounts assigned to an individual.* • *The creation, modification and deletion (life cycle) of user accounts is performed trough IT. For this purpose, the following action is performed/procedures are set up:* • *- Unique and personalized user accounts are used.* • *- The use of ""collective accounts"" is regulated and are minimized. (Lab accounts only) - User accounts are disabled immediately after the user resigns from or leaves Sciosense.* • *- User accounts are checked regularly.* • *- Login credentials are provided to the user in a secure manner.* • *- Admin Accounts are personalized* • *- A policy for handling login data is established and implemented. The following aspects are considered:* • *- No disclosure of login data to third parties - even to persons with authority - subject to legal restrictions* • *- login data must not be written down or stored unencrypted.* • *- immediate change of login data if a possible compromise is suspected.* • *- modification of temporary or initial login credentials after initial login* • *- requirements for quality of login credentials (Strong passwords are mandatory and enforced by technical policy)* • *- The login credentials (e.g., passwords) of a personalized user account must be known only to the assigned user. - A basic template for user accounts with minimum access rights and functions is defined and used.* • *- Sciosense User accounts are created or authorized by the responsible authority within Sciosense.* • *- User accounts of service providers are blocked/deleted upon completion of their task.* • *- Deadlines are set for blocking and deleting user accounts, by configure an expiry date as soon it is known + Ticket.* • *- The use of default passwords is made technically impossible. (strong authentication)* • *- User accounts are checked at regular intervals.* • **The following documents were checked during the assessment:** *Technical Security Policy,* • *Chapter 4 : 4. Policies for Access Security (A.9)* • *Cahpter 7 : - 7.4.1 Reporting and monitoring (A.12.4)*

- *Authorization Matrix (Base27 + SAP).*
- *AD & Azure "*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

4.2 Access Management

4.2.1 To what extent are access rights assigned and managed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Access rights are distributed at Sciosense based on the role of the employee. During the on boarding process, the role of the employee indicates which rights he/she is assigned within the systems of Sciosense. The initial permissions are assigned by the minimum principle. Afterwards an approval flow determines (by the employee's supervisor and the internally responsible manager of the assets) who needs additional rights on certain systems/ infromation. After approval, additional rights are granted as needed. The requests and approvals are stored for audit and regular internal checks. Onboarding/Offboarding, "* **The following documents were checked during the assessment:** • *Authority Matrix, (Base27 & SAP)* • *Technical Security Policy* • *chapter 4. Policies for Access Security (A.9)* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**

Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5 IT Security / Cyber Security

5.1 Cryptography

5.1.1 To what extent is the use of cryptographic procedures managed?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"Many encryptions are in use at ScioSense, for example Device-, Transport-, and Fileencryptions. The most encryptions are done with Active Directory based Certificates, public services are secured with public Certificates. For every encryption an own key is in place. Those Keys are stored securely in ActiveDirectory or in our Password Manager. There is an emergency procedure available to restore/replace encryption keys.*
- *Sciosense uses Disk encryption and encryption of Data are ""transported"" via VPN.*
- *For this, the most current standards are used with the highest encryption values. The encryption via VPN applies to the Client as well as to the site 2 site connections between the sciosense sites.*
- *An emergency procedure is available to restore the disk encryptions. (Bitlocker). "*

The following documents were checked during the assessment:

- *Technical Security Policy*
- *chapter 5 Cryptography (ISO27001-A.10)*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.1.2 To what extent is information protected during transport?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"'The Network services used to transfer informastion are identified and documented, organizational and technical policies and procedures are in place and monitored. For example Mail is secured by TLS and SPF, DKIM and monitored by DMARC - high sensitive Mails are encrypted by S/MIME. In addition we have an own SFTP Server secured by SSL running. High sensitive data are encrypted by ZIP encryption in addition. For permanent connections between external parties like our SAPR3 Hoster or Logistic Partner LGI Site to Site VPNs are active using the highest technically possible encryption. For other cases users are aware to use only https secured connections to exchange data.* • *The connections are documented,(If rerquired) regularly checked and audited (twice a year, if applicable"* **The following documents were checked during the assessment:** *Technical Security Policy* • *chapter: 5. Cryptography (ISO27001-A.10)* • *chapter 8. Communication security (A.13)* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.2 Operations Security

5.2.1 To what extent are changes managed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"All changes to the organization, IT systems and business processes, in relation to security, are recorded and carried out by established procedures. (Change procedure - CAB) Changes within the organization, such as new or departing employees, are processed by the on-off boarding procedure. Changes within business processes or IT systems are subordinated to change management (CAB) Information security requirements for changes in the organisation, business processes and IT systems have been established and are applied after approval of the CAB. These changes are evaluated to what extent they affect the security requirements. For each major change, a roll-back scenario is set up to avoid potential disruptions and risks"* **The following documents were checked during the assessment:** *CAB, Change Management Procedure, Technical Security Procedure* • *chapter 7.1.1. Change management (ISO27001-A.12.1.2)* • *chapter 9.1.1. Analysis and specification of security* • *requirements (ISO27001 - A.14.1.1)* **The following MUST-requirements have been verified during the assessment:** • Control of documents, whether information security requirements for changes to the organization, business processes, IT systems are determined and applied. **The following SHALL-requirements have been verified during the assessment:** • Control of documents, whether a formal approval procedure is established. • Control of documents, whether changes are checked and evaluated for potential impacts on information security. • Control of documents, whether changes affecting information security are planned and tested. • Control of documents, whether procedures for fall-back in fault cases are taken into account. **The following HIGH-requirements have been verified during the assessment:**

- Control of documents, whether compliance with the information security requirements is verified during and after the changes are applied.

The following further information was documented during the assessment:

Once a months there is a CAB meeting. All new changes are introduced and discussed there. A list of older changes from the past was presented.

ScioSense presented an content presentation of the last CAB meeting.

Finding

Based on the observations, no deviation was found.

5.2.2 To what extent are development and testing environments separated from operational environments?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"By determining which devices are ""sensitive"" within Sciosense, development equipment and development environments are technically separated from the office network. (Network segmentation).*
- *Spaces where sensitive equipment is worked on are included in the access protocol so that only employees who, in their sciosense role, are allowed to be in these test environments, can enter. Furthermore, only ""Lab"" accounts are used on development machines. Only information system SAP , is a 2 tier system . Technical Security Policy (A.14), SAP 2-tier :*
- *Non applicable for Sciosense Sensor dev.*

The following documents were checked during the assessment:

Technical Security Policy (A.14)

- chapter: 9.2.1. Policy for secure development (ISO27001- A.14.2.1

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.2.3 To what extent are IT systems protected against malware?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Within Sciosense, the following technical and orgainiastorical measures have been taken to protect against Malware:* • *- THe use of (everysite clustered) Cisco Firepower Firewalls.* • *- The use of Cisco umbrella (Service) to shield oneself from accessing sites and site content that are ""not wanted"".* • *- The use of a malware/ virus and phishing filter at Microsoft where all incoming mail is screened.* • *- The use of MS 365 Defender & MS Endpoint protection on all all Clients.* • *- TrendMicro Client on all Servers..* • *- MS 365 Defender on all devices. (Clients/servers)* • *- Cisco Umbrella on all devices. (Clients/servers)* • *- Dartrace to monitor all incoming mails* • *- Dartrace to monitor sucpicence user/ device behaivior (based on AI learning)* • *- All users / devices are by group policies where it is not possible to disable or uninstall Defender / Umbrella. Systems that are Out of Service - for example old Operating Systems, are separated into deticated Networks or completely without Network.* • *- Sciosense uses learning portals to raise awareness among Sciosense employees and holds regular team meetings where security is regularly discussed and employees are informed.* • *"* **The following documents were checked during the assessment:** *Technical Security Policy.* • *chapter: 7.2. Protection against malware (A.12.2)* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence

The following aspects are based on the plausibility check: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.2.4 To what extent are event logs recorded and analyzed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Within ScioSense, logging is carried out at various levels.* • *Technical logging on: Firewalls & Switches (active network components), Sciosense monitoring, servers and within the Sciosense Office365/ Azure portal. Sciosense does not have a NOC (Network Operations Center). (Scale). Logging on technical level is therefore mostly reactive instead of proactive. As we do not have a NOC Sciosense use Firesight Management Centre to monitor the Firewall, logging of Firewall data is done on a separate Syslog Server for Firewall Events. The most importants Events on Clients are logged on the Asset Management (Lansweeper). In Addition Darktrace is monitoring the Network Traffic on all Sites and logging the activities.* • *Organizational: all incidents are logged in the Sciosense Helpdesk application. Logging also takes place on incidents that need to be reported to local authorities in case of data protection, business security and information security incidents."* **The following documents were checked during the assessment:** *Technical Security Policy* • *chapter: 7.4.1. Recording events (log files) (ISO27001 -A.12.4.1)* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**

Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.2.5 To what extent are vulnerabilities identified and addressed?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"For Sciosense IT vendors, that are involved in any information security, NDA's are agreed & signed, and contracts are in place for the relevant requirements and responsibility's. Also agreements are made about shared responsibility's and the implementation as such. Patch management is done by Supplier and Sciosense IT. (WSUS) With Microsoft Endpoint Management and Defender we are getting notifications about known vulnerabilities. After getting such notification the needed action is considered and taken. We have OS Patchmanagement with WSUS and Application patching by Endpoint Management. With Lansweeper we can run a report to verifiy if all systems been patched successful "* **The following documents were checked during the assessment:** *Technical Security Policy* • *chapter: 7.5. Technical vulnerability management (A.12.6)* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.2.6 To what extent are IT systems technically checked (system audit)?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"Sciosense equipment is the responsibility of Sciosense IT in conjunction with an external IT supplier. It has been contractually agreed with them that systems will be audited once a quarter.*
- *It has been contractually determined which audits will be performed and how they will be carried out.*
- *This ranges from system checks, data backup to data integrity checks an security audits. These audits are reported and evaluated Quarterly with the SDM (Service Delivery Manager) and any corrective actions taken.*
- *Reports are kept for evaluation, review and audit purposes.*

- *Sciosense also uses an extensive proprietary monitoring system (PRTG) in which not only systems are monitored but also important services that are important for the business of Sciosense. Sciosense Monitoring is the responsibility of ScioSense IT and is done real time so that any major disruption can be immediately resolved or changes can be initiated. In Addition ScioSense IT is taking regual checks of most important Systems / Configurations (ISMS- Base27) Technische controles,*
- *LAN sweeper*
- *PRTG (Availability checks)*
- *External audits (Leitwerk, Routz) "*

The following documents were checked during the assessment:

- *ISMS- Base27*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.

• Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.2.7 To what extent is the network of the organization managed?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"Within Sciosense a network plan is present that prescribes the segmentation of the network. Network Devices are categorized and in dedicated grouped Networks.*
- *This segmentation plan is taken into account during the installation but also during expansions of the Sciosense network. External Network services are only accessible through a DMZ (DeMilitarized Zone) that is located in the Sciosense IT supplier's data center. Cisco Firepower Firewalls are installed at all Sciosense locations including the data center and are controlled by the central Firesight Management Centre. This is currently done reactively. Connections to IT service providers are done with vpn and high encryption. The monitoring of the Firewall is done by the IT supplier (contracts) and actively moniored by Darktrace for intrusion detection and prevention and unintended data exchange.*

- *PRTG. Sciosense Monitor"*

The following documents were checked during the assessment:

Technical Security Policy

- *chapter: 8.1. Network security management (ISO27001- A.13.1)*
- *chapter: 4.1.2. Access to networks and network services (ISO27001-A.9.1.2)*
- *chapter: 7.4.1. Recording events (log files) (ISO27001- A.12.4.1)*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.3. System acquisitions, requirement management and development

5.3.1 To what extent is information security considered in new or further development of IT systems?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"The information security requirements related to Sciosense infrastructure are determined and applied when acquiring or expanding the Sciosense landscape.* • *The following requirements must be met within Sciosense:* • *- The IT system is tested for compliance with the specifications drawn up by Sciosense before productive use.* • *- The specifications are checked against the information security requirements.* • *Information security requirements are taken into account before and during implementation of ScioSense equipment.* • *Because Sciosense uses test equipment for Research & Development, the data on these systems are considered confidential and therefore falls within the Sciosense security policy. CAB"* **The following documents were checked during the assessment:** • *Supplier Policy* • *Technical security procedure* • *Sciosense security policy* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.3.2 To what extent are requirements for network services defined?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Requirements regarding the information security of network services are determined and fulfilled.* • *Agreed SLAs with the service provider and internal apply here.* • *A redundant service is set up on every Sciosense site that takes over in case of any disruption.* • *This applies to network services as well as redundant availability of data within the Sciosense network.* • *Data Classification,* • *CAB* • • *preferred suppliers: Dell, Cisco, Microsoft, Leitwerk, Routz, Veeam."* **The following documents were checked during the assessment:** *Technical Security Policy* • *chapter: 8. Communication security (A.13)* *Technical Continuity Plan,* • *BIA* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level.

• Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.3.3 To what extent is the return and secure removal of information assets from external IT services regulated?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"A procedure for returning and securely removing information assets, from an external IT service, (e.g. from external contractors) is established and implemented.* • *Responsibility for the information assets used is contractually defined. Assets used by external service providers are included in the Sciosense asset management system. Returning and securely removing internal informations assets are part of the off-boarding procedure or in the Device Lifecycle policy. Contract met Leitwerk (DPA see supplier Base27) & Ifactive."* **The following documents were checked during the assessment:** • *Device Lifecycle policy* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

5.3.4 To what extent is information protected in shared external IT services?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *"Within Sciosense, we do not have external tenants from other (external) companies. Where this does occur with IT vendors, contractual agreements are and/ or NDAs are in place and pysical separation like : Own cabinet at Leitwerk, own cabinet in Eindhoven (shared server room).* • *For Leitwerk see document (supplier) for Floorplan Datacenter."* **The following documents were checked during the assessment:** • *SC-001860-PN Floorplan Sciosense IT rooms & access.pdf* **The following aspects were taken into account during the plausibility check of this control:** • Existence and scope of the description of the self-assessment • Presence of a degree of maturity • Availability of the specified reference documentation • Viewing and checking the specified evidence **The following aspects are based on the plausibility check**: • Conclusion that the self-selected maturity level corresponds to the required target maturity level. • Conclusion that a general plausibility of the control can be confirmed. **Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.**
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

6 Supplier Relationships

6.1.1 To what extent is information security ensured among suppliers and cooperation partners?

Detailed Description (Including Assessment Procedure)
The evaluation of the controls is based on: ☒ Interviews ☐ Onsite inspection ☒ Document inspection ☒ Check of the implementation (evidences) **The auditee did provide the following comment within the self-assessment:** • *" At ScioSense we are using Contracts, DPAs, SLA's and NDA's as organizational security. In Addtition our users are trained to be aware about what kind of informations can be shared with the external party* • *"* **The following documents were checked during the assessment:** • *Supplier policy,* • *NDA's,* • *Specific contracts,* • *SLA,s.,* • *BIA* • *Supplier checks* **The following MUST-requirements have been verified during the assessment:** • Implementation check, whether suppliers and cooperation partners are subjected to a risk assessment with regard to information security. • Implementation check, whether an appropriate level of information security is ensured by contractual agreements with suppliers and cooperation partners. • Control of documents, whether ,where applicable, contractual agreements with customers are passed on to suppliers and cooperation partners. • Control of documents, whether compliance with contractual agreements is verified. **The following SHALL-requirements have been verified during the assessment:** • Implementation check, whether suppliers and cooperation partners are contractually obliged to pass on any requirements regarding an appropriate level of information security also to their subcontractors. • Control of documents, whether service reports and documents by suppliers and cooperation partners are reviewed. **The following HIGH-requirements have been verified during the assessment:**

- Implementation check, whether evidence that a supplier's level of information security is adequate for the protection needs of the information (e.g. certificate, attestation, own audit) is provided.

The following further information was documented during the assessment:

All supplier are listed with their available information security certificates (f.e. ISO, TISAX). ScioSense always performes a BIA for every supplier and estimatates the risk for working together with a supplier.

Finding

Based on the observations, no deviation was found.

6.1.2 To what extent is non-disclosure regarding the exchange of information contractually agreed?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"See also 6.1.1.*
- *A Sciosense Non-disclosure (NDA) agreements contain the following information:*
- *- the persons/organization(s) involved,*
- *- the nature of the information covered by our agreement,*
- *- the subject matter of the agreement*
- *- the duration of the agreement (temporary or permanent)*
- *- responsibilities*
- *- provisions for the handling of sensitive information outside the contractual relationship. (such as 3th party contractors)*

- *A process for monitoring the validity of temporary non-disclosure agreements and for timely initiation of their renewal is in place.*
- *The requirements and procedures for the application of NDA and the handling of sensitive information are regularly reviewed.* *,*
  "

The following documents were checked during the assessment:

- *Suppliers: BIA score based, Employees: Labour Contract*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.
Finding
AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.

7 Compliance

7.1.1 To what extent is compliance with regulatory and contractual provisions ensured?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☒ Interviews ☐ Onsite inspection ☒ Document inspection ☒ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"Where this takes place with IT suppliers, contractual agreements have been made or NDAs are in place. These contracts or NDAs establish compliance with the requirements and are communicated to the responsible persons.*
- *Regular sessions are organized and information is made available to raise staff awareness of information security compliance issues. Compliance to regulatory statutes related to information security and information technology is checked annually. Contractual provisions are reviewed once per year and based on inputs from various disciplines, contractors are informed of their compliance/non-compliance Contract & NDA's refer to applicable regulatory requirments when nessasary."*

The following documents were checked during the assessment:

- *NDA's, Labour contracts, BIA, Supplier Checks*

The following MUST-requirements have been verified during the assessment:

- Implementation check, whether legal, regulatory and contractual requirements and specifications of relevance to information security (see examples) are regularly determined.
- Control of documents, whether policies regarding compliance with the requirements are defined, implemented and communicated to the responsible persons.

The following SHALL-requirements have been verified during the assessment:

- Control of documents, whether the integrity of records in compliance with contractual, regulatory or legal obligations and business requirements are taken into account.

The following further information was documented during the assessment:

ScioSense presented a list of identified laws for every location/country.

Finding

Based on the observations, no deviation was found.

7.1.2 To what extent is the protection of personal data taken into account when implementing information security?

Detailed Description (Including Assessment Procedure)

The evaluation of the controls is based on:

☐ Interviews ☐ Onsite inspection ☒ Document inspection ☐ Check of the implementation (evidences)

The auditee did provide the following comment within the self-assessment:

- *"Within Sciosense,we have Register of processing activities, Processing agreements with suppliers/thirdparties that process personal data on our behalf. Further additional requirements to suppliers that process personal data are defined based on the supplier policy. Within Sciosense we follow the GDPR in which a Sciosense procedure states how we deal with the protection of personal data. Within this procedure, the following is taken into account:*
- *- Information security requirements relating to the procedures and processes in the processing of personal data are established.*
- *- Compliance requirements for the protection of personal data are established and known to the persons to whom the data are entrusted.*

- *- The rules of compliance for the protection of personal data are documented and known to the persons to whom the data is entrusted.*
- *- The management system (ISMS) takes into account the processes and procedures for the protection of personal data."*

The following documents were checked during the assessment:

- *BIA, Processing overview, Data classification, Privacy Policy, supplier policy.*

The following aspects were taken into account during the plausibility check of this control:

- Existence and scope of the description of the self-assessment
- Presence of a degree of maturity
- Availability of the specified reference documentation
- Viewing and checking the specified evidence

The following aspects are based on the plausibility check:

- Conclusion that the self-selected maturity level corresponds to the required target maturity level.
- Conclusion that a general plausibility of the control can be confirmed.

Based on the descriptions available, the control is considered plausible. Further interviews were therefore not carried out for this control.

Finding

AL2: The description of the implementation in relation to the evidences provided is ☒ plausible ☐ not plausible.